Deutscher Bundestag
13. Wahlperiode

Drucksache 13/5777

11. 10. 96

Antrag

der Abgeordneten Dr. Manuel Kiper, Elisabeth Altmann (Pommelsbrunn), Manfred Such, Rezzo Schlauch und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Ein ökologischer, sozialer und demokratischer Weg in die Informationsgesellschaft III (Schutz und Entfaltung selbstbestimmter Nutzung)

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die mit dem Wandel zur Informationsgesellschaft verbundenen gesellschaftlichen, politischen, wirtschaftlichen und kulturellen Veränderungen sind tiefgehend. Kaum jemand wird von diesen Veränderungen nicht betroffen sein. Allein wirtschaftliche Gesichtspunkte in den Mittelpunkt zu stellen, wird jedoch dazu führen, die in digitalen Technologien enthaltenen Potentiale weder unter betriebswirtschaftlichen Aspekten und schon gar nicht unter Aspekten innovativer und selbstbestimmter Nutzung auszuschöpfen. Das gern als Modell angeführte Internet verdankt seine Attraktivität allein einer aus nichtkommerziellen Zwecken sprießenden Vielfalt an Meinung und Information. Die Weiterentwicklung derartiger Aktivitäten einer Vielzahl von Personen durch eine verstärkte Kommerzialisierung zu behindern statt zu fördern, wäre ein herber Verlust für die Gesellschaft, der aber auch die Wirtschaft beträfe. Die Entwicklung zu einer Informationsgesellschaft ist nur dann tragbar, wenn sie auf demokratischen Grundwerten beruht. Besonders der Schutz der Persönlichkeitsrechte und die Weiterentwicklung des Datenschutzes, die Entfaltung einer informationellen Grundversorgung und eine Gestaltung auf demokratischem und partizipativem Wege müssen dabei im Vordergrund stehen.

Die Informationsgesellschaft, wie sie dagegen als Leitbild von der Bundesregierung vertreten wird, ist mit bemerkenswerten Unsicherheiten behaftet. Seit der Vorlage eines grundlegenden Antrages zu Maßstäben und Grundlagen der Gestaltung der Informationsgesellschaft durch die Fraktion BÜNDNIS 90/DIE GRÜNEN (Drucksache 13/3010) haben sich bereits eine Reihe der zum damaligen Zeitpunkt von der Bundesregierung vertretenen Ansichten als unbegründet herausgestellt. Die Hoffnungen auf zahlreiche neue Arbeitsplätze und ökologische Potentiale wurden gedämpft. Die Aussichten auf neue demokratische und partizipative Impulse durch wesentlich verbesserten Zugang zu Informationen hat die Bundesregierung selbst am deutlichsten in Frage

gestellt. Wie eine Konferenz der Bundesregierung zu den Werten der Informationsgesellschaft jüngst zeigte, geht es ihr nunmehr vor allem um den Markt, der sich durch neue Produkte und vor allem Dienstleistungen im Zusammenhang mit digitalen Diensten auftun soll.

Der Markt aber hat bisher das heute erreichte Informationsangebot auf elektronischen Netzen nicht hervorgebracht. Ob er dies in Zukunft unterstützt oder behindert, wird den Erfolg der Investitionen ausmachen, die viele Anbieter neuer Informationsdienstleistungen heute tätigen. In der Informationsgesellschaft werden die Spielregeln des Datenzugangs andere sein als heute. Noch bestimmt auf elektronischen Netzen derjenige die Entwicklung, der den Informationsfluß am wenigsten hemmt. Umfassende Meinungsfreiheit und nichtexistente Zensur sind Kennzeichen demokratischen Selbstbewußtseins in einem eigenverantwortlich und dezentral koordinierten Kommunikationsmedium. Eine selbstbestimmte Nutzung kann sich nur entfalten, wenn dies auch so bleibt und nicht durch obrigkeitsstaatlich anmutende Bevormundung ersetzt wird. Wenn dieses Medium nun zu einem neuen Markt wird, sollte auch klar sein, daß ein Markt, auf dem die Rechte der Kundinnen und Kunden kaum gelten und ihre Daten ungenügend geschützt sind, sich nicht entwickeln kann. Informationsdienstleistungen, über die vor allem im Zusammenhang mit der Verbreitung gesetzwidrigen Materials debattiert wird, sind – obwohl die Bundesregierung selbst erklärt, über 99 % des beispielsweise auf dem Internet verfügbaren Materials sei in Einklang mit deutschem Recht – kein Anreiz für eine breitere Nutzung. Eine Lösung besteht aber nicht darin, den Rest von unter 1 % auszumerzen, sondern eine kompetente Nutzung dieser neuen Angebote als Medienkultur zu entwickeln und zu vermitteln.

Noch bevor das Internet als Arbeitsmittel und als organisatorische Infrastruktur für Unternehmen und die öffentliche Verwaltung in einem breiteren Umfang Bedeutung erlangt, findet seine Umwandlung zum Marktplatz statt. Doch die Schutzrechte all jener, die diesen Marktplatz aufsuchen wollen, sind kaum entwickelt. Mit dem Verweis auf die weltweite Natur dieses Marktplatzes wird gern begründet, daß nationale Regelungen unmöglich seien. Eine solche Argumentation zeugt entweder von Unkenntnis oder verweigert sich bewußt der Mühe, genauer zwischen regelbaren und nicht regelbaren Sachverhalten zu differenzieren und zu erläutern, wo auch für national nicht regelbare Aspekte Lösungsansätze möglich sind, in denen die Kundinnen und Kunden einen gewissen Schutz eigenverantwortlich herstellen können.

Mit dem Telekommunikationsgesetz (TKG) wurde versucht, den Schutz von Persönlichkeitsrechten auf der Ebene zu normieren, auf der der telekommunikative Zugang zu Informationsangeboten aller Art stattfindet. Dieser Versuch ist allerdings in den wichtigsten Teilen mißglückt. Die Bundesregierung blieb deutlich hinter dem zurück, was als Mindestvoraussetzung einer ökologischen, sozialen und demokratischen Informationsgesellschaft als Schutz der Persönlichkeitsrechte und des Fernmeldegeheimnisses notwendig gewesen wäre und als Alternative deutlich formuliert wur-

de (vgl. Drucksache 13/4892). Die Basis einer informationellen Grundversorgung als entsprechende Ausgestaltung eines Universaldienstes zu regeln, wird mittlerweile zwar von der EU-Kommission durchaus gesehen (vgl. Kom [96] 73 endg.), die Regelung im TKG wird dem jedoch nicht annähernd gerecht. Von den Regelungen im TKG unberührt blieb die Nutzung all jener Dienste und Angebote, die für den Markt von Informationsdiensten kennzeichnend sind.

Eine Regelung zum Schutz der Kundinnen und Kunden wurde nicht zuletzt dadurch erschwert, daß in Bund und Ländern unterschiedliche Auffassungen über die Klassifikation der heute und in absehbarer Zukunft möglichen Dienste herrschen. Es ist nicht absehbar, wie die getroffenen Vereinbarungen der heute schon sichtbaren Dienstevielfalt standhalten sollen. Technisch wollen einerseits z. B. TV-Kabelanbietergesellschaften über ihr Kabel Internet-Dienste einschließlich Telefonie mit beliebigen Teilnehmern per Internet anbieten. Andererseits ist das laufende Fernsehprogramm von 20 Kanälen via Internet verfügbar. Es ist derzeit nicht auszuschließen, daß derselbe Dienst – sei es der Zugang zum Fernsehprogramm oder das Telefonieren – von Bund und Ländern in unterschiedlichen Rechtszusammenhängen und mit unterschiedlich hohen Schutznormen geregelt wird. Dabei ist es dringend erforderlich, daß unabhängig von der Zuständigkeit für einzelne Dienste – ob Bund oder Länder – dieselben hohen Schutznormen gelten. Die Zuständigkeit mißt sich an der Unterscheidung zwischen Individual- oder Massenkommunikation. Doch für den Datenschutz und die Informationelle Selbstbestimmung ist es gleichgültig, ob z. B. abrufbare Filmsequenzen wie Video-on-Demand oder Pay per View unter die rundfunkrechtliche Länderkompetenz fallen, Email und Telebanking als individuelle Kommunikation dagegen unter das Bundesrecht fallen.

Anbieter müßten unterschiedliche Rechtsnormen in ihren verschiedenen Teilsystemen beachten und umsetzen sowie die dafür entstehenden Kosten tragen. Gravierende Nachteile entstehen jedoch vor allem für Kundinnen und Kunden, wenn sie nicht einmal sicher von der Geltung konkreter Rechtsnormen für die von ihnen gewählte Form digitaler Dienste ausgehen können und die verbleibenden Rechtsunsicherheiten zu tragen haben. Die Folge solch unklarer Normen wäre eine dysfunktionale Regulierung ohne Rechtssicherheit für Kundinnen und Kunden einerseits und Anbieter andererseits. Eine derartige Dysfunktionalität behindert digitale Dienste.

Die Bundesregierung ist daher gefordert, einen einheitlichen Rahmen zum Schutz der Rechte von Bürgerinnen und Bürgern in der Informationsgesellschaft zu entwickeln und im Einvernehmen mit den Ländern zu normieren. Solange die Adaption insbesondere des Informationellen Selbstbestimmungsrechts und des Datenschutzes, der Meinungsfreiheit, der Vielfalt und des Pluralismus sowie des freien Informationszugangs, des Verbraucherschutzes und anderer bestehender Rechte an die Nutzung digitaler Dienste nicht erfolgt ist, wird es keine Basis für eine rechtsstaatlich fundierte Informationsgesellschaft geben.

II. Der Deutsche Bundestag fordert die Bundesregierung auf:

A. Datenschutz und Fernmeldegeheimnis

1. Ein einheitlicher Schutz von Daten ist umfassend für alle Dienste zu normieren, bei denen individuelle Kundendaten erfaßt werden und bei denen nicht nur Anbieter Daten an Kunden übertragen, sondern auch eine umgekehrte Datenverbindung vorhanden ist.

2. Für die von den Nutzerinnen und Nutzern aller digitalen Dienste erhobenen Daten hat das Minimierungsgebot zu gelten. Die genutzte Technik ist grundsätzlich derart zu gestalten, daß möglichst wenige personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Die Erhebung von Nutzungs- und Verbindungsdaten ist auf das für die Leistungserbringung absolut notwendige Maß zu begrenzen. Die Speicherung ist bei Nutzungsdaten nur bis zum Ende der Verbindung, bei abrechnungsrelevanten Verbindungsdaten nur bis zum Ende der Einspruchsfrist nach Rechnungslegung statthaft. Die Bundesregierung hat klarzustellen, daß es sich bei Verbindungsdaten nicht um Geschäftsunterlagen mit entsprechenden langjährigen Aufbewahrungsfristen handelt.

3. Das Fernmeldegeheimnis ist seiner Bedeutung als strategisches Grundrecht der Informationsgesellschaft entsprechend auszubauen. Notwendig ist auch ein Mediennutzungsgeheimnis, das die Bürgerinnen und Bürger vor einer Überwachung ihres Mediennutzungsverhaltens schützt. Bestehende Verschwiegenheitspflichten, Zeugnisverweigerungsrechte und Beschlagnahmeverbote sind den Entwicklungen zu elektronischen Transaktionsformen anzupassen.

4. Eine Übermittlung von Daten an Dritte ist zu untersagen. Ausnahmen hiervon betreffen lediglich Daten, die für die Abrechnung kostenpflichtiger Dienste Dritter notwendig sind und für deren Nutzung eine ausdrückliche Einwilligung des Nutzers vorliegt. Nutzungsprofile sind nicht zu gestatten. Dies ist bereits bei der Gestaltung der Systeme zu berücksichtigen und durch Datenschutzkontrollen effektiv zu gewährleisten.

5. Nutzerinnen und Nutzern von Informationsdiensten ist die Nutzung von Diensten in anonymer Form, wo immer dies möglich ist, und die Nutzung pseudonymer Nutzerkennungen wahlfrei zu ermöglichen. Die Nutzung von anonymisierenden Diensten und Systemen zur selbstbestimmten Kontrolle übermittelter Daten bleibt frei von Einschränkungen und Zugangsbeschränkungen.

6. Digitale Dienste erfordern eine anlaßunabhängige und effektive Datenschutzkontrolle. Da die neuen Regelungen sowohl für private als auch für öffentliche Stellen gelten müssen, ist die überkommene Aufteilung der Datenschutzkontrolle für die beiden Bereiche nicht mehr zeitgemäß; die Kompetenzen der Aufsichtsbehörden für den privaten Bereich sollten an die Datenschutzbeauftragten übertragen werden.

7. Die Bundesregierung wird aufgefordert, auf internationaler Ebene keiner Einschränkung des bundesdeutschen Datenschutzrechts zuzustimmen. Statt dessen sind grenzüberschreitende Datenschutzkontrollinstanzen einzurichten, die gegen Datenschutzverstöße effektiv vorgehen können. Sofern dieser Schutzstandard nicht zügig erreicht wird, ist zu prüfen, ob als zusätzliche Schutzmaßnahme – parallel zur Verfolgung des Ziels eines international wirksamen Datenschutzes – das Copyright dahin gehend weiterzuentwickeln ist, jeder Person ein Copyright an ihren personenbeziehbaren Daten zu geben.

8. Den Datenschutzbeauftragten sind für die beschwerdeunabhängige Beobachtung der Entwicklung bei der Nutzung personenbeziehbarer Daten in internationalen elektronischen Netzen, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Beobachtung der in diesen beobachtbaren Gefahren für die IT-Sicherheit angemessene Mittel bereitzustellen. Beide haben über in den jeweiligen Bereichen erkannte Probleme zeitnah und über die allgemeine Entwicklung regelmäßig die Öffentlichkeit zu informieren.

B. Schutz der Verbraucherinnen und Verbraucher

1. Die Bundesregierung wird aufgefordert, einen Verbraucherschutz zur Grundlage aller digitalen Dienste zu erarbeiten, der den bei herkömmlichen Geschäften erreichten Stand auch für diese Dienste sichert.

2. Jede Form digitaler Dienste ist zu Preistransparenz zu verpflichten. Der Abruf kostenpflichtiger Dienste ist vorab deutlich und von einer eindeutigen und spezifischen Willensbekundung abhängig zu machen, ein Stornieren oder Widerrufen des Abrufs muß ermöglicht werden. Die entstandenen Kosten sind den Kundinnen und Kunden jederzeit anzuzeigen.

3. Die Bundesregierung wird aufgefordert, die Aufhebung minimaler Standards in den Geschäftsbedingungen zu unterbinden und die Bekanntmachung von Geschäftsbedingungen digitaler Dienste so zu regeln, daß eine Gültigkeit erst dann gegeben ist, wenn sie den Kundinnen und Kunden in unveränderbarer Form zugegangen sind.

4. Die Bundesregierung hat die Haftungsregelungen den Bedingungen digitaler Dienste anzupassen. Insbesondere sind dabei solche Haftungsbeschränkungen für nichtig zu erklären, die mit systembedingten Unzulänglichkeiten begründet werden.

5. Die Bundesregierung wird aufgefordert, bei Informationsdienstleistungen den Wohnort von Kundinnen und Kunden zum rechtlichen Erfüllungsort von kommerziellen Informationsdienstleistungs-Angeboten zu machen.

6. Die Bundesregierung hat die rechtlichen Grundlagen dafür zu schaffen, daß Anbieter von Informationsdienstleistungen ein besonderes Gütesiegel für die Nutzung qualitativ herausragender Produkte und Systeme sowie für den effektiven Schutz personenbezogener Daten führen können. Dabei ist zu prüfen,

inwieweit sich die Zertifizierung durch das BSI in diesem Sinne erweitern läßt.

C. Informationszugang und Entfaltung

1. Für Anbieter von Informationsdienstleistungen ist keine besondere Zulassung erforderlich.

2. Die Bundesregierung hat bei Regelungen bezüglich Anbietern von Informationsdienstleistungen die Vielfalt kleiner – insbesondere nichtkommerzieller – Anbieter und Privatpersonen zu beachten und zu fördern.

3. Die Bundesregierung wird aufgefordert, der bestehenden Rechtslage Beachtung zu verschaffen, nach der Informationsdienstleister, die einen Zugang zu Angeboten anderer bieten, nicht für die Inhalte auf deren Systemen verantwortlich sind. Die Bundesregierung wird darüber hinaus aufgefordert, sich auf internationaler Ebene für die Meinungsfreiheit einzusetzen und Einschränkungen dieses Rechts entgegenzutreten.

4. Zum Schutz der Jugend ist es Aufgabe der Bundesregierung, Bürgerinnen und Bürger über die Gefahren eines freien Informationszugangs und Möglichkeiten der Abhilfe einerseits aufzuklären, andererseits durch internationale Abkommen zur Amtshilfe und ggf. Initiativen zur Angleichung relevanter Straftatbestände den Strafverfolgungsbehörden die rechtlichen Mittel an die Hand zu geben, auch international der Urheber strafbarer, jugendgefährdender und verrohender Materialien habhaft zu werden. Zensurbestrebungen hat die Bundesregierung auf nationaler wie internationaler Ebene entgegenzuwirken.

5. Die Bundesregierung wird aufgefordert, ein Recht auf Akteneinsicht – Recht auf Informationsfreiheit nach dem Vorbild des Freedom of Information Acts der USA – zu entwerfen und eine Novelle des Umweltinformationsgesetzes mit dem Ziel vorzulegen, die Ausnahmen vom Auskunfts- und Einsichtsrecht sowie die Auskunftskosten zu vermindern.

6. Die Bundesregierung wird aufgefordert, Universitäten und Forschungseinrichtungen als Produzenten von Wissen und daraus erstellten Informationen einerseits und das Deutsche Forschungsnetz als Infrastruktur für Zugriff und Verteilung dieser Informationen andererseits in besonderer Weise zu fördern.

7. Jenseits der im Projekt „Schulen ans Netz" erfolgten Ausrüstung einiger Schulen mit Computern und leistungsfähigen Telekommunikationsanschlüssen hat die Bundesregierung in Zusammenarbeit mit den Ländern Mittel dafür bereitzustellen, die für die Vermittlung entsprechender Kenntnisse erforderlichen pädagogischen Konzepte und Fähigkeiten zu erarbeiten und für deren Verbreitung zu sorgen. Bei der Vergabe von Telekommunikationslizenzen und bei der Ausgestaltung des Universaldienstes ist insbesondere darauf zu achten, daß Ausbildungseinrichtungen in besonderer Weise und dauerhaft mit

kostengünstigen und leistungsfähigen Zugängen zu Informationsdiensten ausgestattet werden.

D. Digitale Signatur und Kryptographie

1. Die Vertraulichkeit der Datenkommunikation und die Verbindlichkeit elektronischer Transaktionen ist nur mittels kryptographischer Verfahren zu gewährleisten. Die Vertrauenswürdigkeit derartiger Verfahren würde stark beeinträchtigt, wenn staatliche Stellen einen Zugriff auf geheime Schlüssel hätten oder wenn Verfahren eingesetzt würden, die mit eingebauten Schwachstellen ausgestattet wären. Die Bundesregierung wirkt deshalb darauf hin, zum Schutz der Persönlichkeitsrechte die Nutzung kryptographischer Verfahren in digitalen Diensten zu erweitern, und beschränkt diese nicht durch Normierung auf bestimmte Verfahren. Sie hat auch bei anstehenden internationalen Richtlinien auf die Umsetzung dieser Maßgabe hinzuwirken. Die Bundesregierung hat die Forschung an kryptographischen Verfahren zu intensivieren und die Normung voranzutreiben.

2. Die Bundesregierung hat bei der Einführung der digitalen Signatur davon Abstand zu nehmen, derartig signierten elektronischen Nachrichten einen Dokumentencharakter einzuräumen, ohne abgesicherte Erfahrungen hinsichtlich der Brauchbarkeit abzuwarten.

3. Die für die Erzeugung digitaler Signaturen zugelassenen Algorithmen haben rigiden Sicherheitsanforderungen zu entsprechen, die von unabhängiger wissenschaftlicher Seite begutachtet werden. Der in diesem Zusammenhang zu regelnde organisatorische Rahmen ist den unterschiedlichen Bedürfnissen verschiedener Anwendergruppen entsprechend flexibel zu regeln. Für diesen organisatorischen Rahmen vergebene Lizenzen sind auf fünf Jahre zu begrenzen. Die damit gewonnenen Erfahrungen sind unter den Aspekten der Sicherheit sowie der gesellschaftlichen Auswirkungen wissenschaftlich zu evaluieren. Die Ergebnisse der Evaluation sind nach fünf Jahren zu veröffentlichen und für den weiteren Gesetzgebungsprozeß zu nutzen.

4. Die Nutzung von Verfahren zur Hinterlegung des privaten Teils der Schlüssel kryptographischer Verfahren – sog. Escrow-Verfahren – ist nicht zu verfolgen.

Bonn, den 11. Oktober 1996

Dr. Manuel Kiper,
Elisabeth Altmann (Pommelsbrunn)
Manfred Such
Rezzo Schlauch
Joseph Fischer (Frankfurt), Kerstin Müller (Köln) und Fraktion

Begründung

Zu A. Datenschutz und Fernmeldegeheimnis

Die einheitliche Eigenschaft digitaler Dienste besteht in der individuellen Anpaßbarkeit des Informationsangebotes. Dies gilt gleichermaßen für Video-on-Demand, bei dem der Zeitpunkt des Medienkonsums individuell gesteuert wird, wie für Internet-Angebote, bei denen Nutzerinnen und Nutzer völlig frei über die Angebotsauswahl bestimmen können.

Diese Anpaßbarkeit wird bei allen Diensten über die Erfassung der Kundenwünsche und -anforderungen hergestellt. Zu diesen Zwecken werden Daten der Nutzerinnen und Nutzer individuell erhoben und verarbeitet. Derartige Daten haben aufgrund ihrer situativen Aussagekraft einen hohen Wert für zielgruppenspezifische, sogar individuell zugeschnittene Werbung und andere Formen kommerzieller Datennutzung. Sie lassen sich leicht zu Nutzungs- und Persönlichkeitsprofilen verdichten. Nutzungsprofile bergen für den Datenschutz und die unbeobachtete und selbstbestimmte Nutzung digitaler Dienste erhebliche und mit dem Recht auf Informationelle Selbstbestimmung unvereinbare Gefahren.

Die Bundesregierung ist gefordert, dem Recht auf Informationelle Selbstbestimmung in digitalen Diensten zur Geltung zu verhelfen. Dies bedeutet nicht, in die Gesetzgebungskompetenz der Länder bei der Regulierung von Video-on-Demand-Angeboten einzugreifen, sondern die Rahmenbedingungen für Kundinnen und Kunden dieser Dienste einheitlich zu fassen. Die Bundesregierung wird daher aufgefordert, im Einvernehmen mit den Ländern solche einheitlichen Regelungen zu normieren, um Nutzungsprofile von Kundinnen und Kunden zu verhindern. Sofern dies nicht einvernehmlich möglich ist, hat sie zu prüfen, ob die zum Zwecke der Diensteauswahl notwendigen Datenübertragungen nicht unter dem Gesichtspunkt der Telekommunikation zu regeln sind, da die Kundendaten in jedem Fall – nicht nur bei Internet-Providern, sondern beispielsweise auch von Set-top-Boxen bei Video-on-Demand-Angeboten – individuell und leitungsgebunden übertragen werden und damit auch unabhängig von Inhalten der Angebote regulierbar sein können.

Die Auswertung von Nutzungs- und Persönlichkeitsprofilen ist nur dann möglich, wenn die dafür nötigen Daten vorhanden sind. Nur die konsequente Minimierung der Daten ermöglicht eine selbstbestimmte Nutzung digitaler Dienste und verhindert Nutzungsprofile. Die Sammlung von Daten ist daher auf das Maß zu beschränken, das zur Erbringung der Dienste absolut notwendig ist. Die angebotenen Dienste sind so zu gestalten, daß der Bedarf an Nutzungs- und Verbindungsdaten so gering wie möglich ist. Sämtliche Daten sind sofort zu löschen, sobald sie nicht mehr für Abrechnungszwecke notwendig sind. Datenübermittlungen an Dritte sind grundsätzlich unstatthaft, sofern sie nicht zur Abwicklung von Abrechnungen von Diensten nötig sind, die Kundinnen und Kunden bewußt und unter Kenntnis der Kosten in Anspruch genommen haben.

Teledienste wie Telemedizin, Telebanking oder Telearbeit nutzen vernetzte Computer zum Austausch sensibelster Daten. Arzt-, Bank- und Betriebsgeheimnis und andere Schutz- und Verschwiegenheitsrechte werden dabei auf den Schutz des Fernmeldegeheimnisses reduziert. Das Fernmeldegeheimnis wird in der Informationsgesellschaft zum strategischen Grundrecht. Seine Wahrung müßte deshalb einen besonderen Stellenwert haben. Gesetzesnormen, bei denen an Sicherheitsbehörden etwa über Telebanking-Kunden Auskünfte gegeben werden müssen, die unter den Bedingungen des Bankgeheimnisses unzulässig wären, sind eine nicht hinnehmbare Aushöhlung von Schutzrechten.

Obwohl im Grundgesetz besonderem Schutz unterworfen, wird derzeit nur die Weitergabe unbefugt erlangter Inhalte von Fernmeldevorgängen bestraft, nicht jedoch deren unbefugte Kenntnisnahme und Nutzung. Ebenfalls zu wenig geschützt ist zudem die Nutzung von Verbindungsdaten, die keine Inhalte sind, aber Auskunft über das Kommunikationsverhalten geben. Diese Verbindungsdaten sind durch Erfassung und Speicherung bei digitaler Vermittlungstechnik zu sensitiven Daten geworden. Das Fernmeldegeheimnis ist deshalb wirkungsvoll und umfassend zu schützen und den technischen Entwicklungen anzupassen.

Informationsdienstleister bieten Zugang zu Angeboten, bei denen weder ein direktes Vertragsverhältnis zu den Nutzerinnen und Nutzern besteht, noch erkennbar ist, ob und in welchem Umfang Daten gesammelt werden. Schutz bietet hier eine auf die Nutzung von Pseudonymen zugeschnittene Organisation der Informationsdienstleister und die Nutzung zusätzlicher Dienste zur technischen Realisierung von Anonymität. Nutzerinnen und Nutzern ist freizustellen, ob und in welchem Zusammenhang sie eine pseudonyme oder anonyme Nutzung vorziehen. Anbieter von Informationsdienstleistungen haben pseudonyme Zugangsmöglichkeiten vorzuhalten. Der Zugang zu Diensten und Systemen, die eine anonyme Nutzung ermöglichen, ist zu unterstützen und nicht durch Regelungen einzuschränken.

Der Schutz der Kundinnen und Kunden benötigt effektive Kontrollinstanzen. Der Datenschutz wird derzeit dadurch erschwert, daß die Aufteilung zwischen privaten und öffentlichen Stellen nicht länger zeitgemäß ist. Die wachsenden Aufgaben verlangen hier eine Bündelung bei den Datenschutzbeauftragten. Kennzeichen von Informationsdiensten ist außerdem die Internationalisierung des Datenverkehrs. Um das bestehende Recht nicht ad absurdum zu führen und hier bestehende Normen zu schützen, kann dies nur durch eine Internationalisierung der Datenschutzkontrollinstanzen effektiv kontrolliert werden. Diese Internationalisierung kommt jedoch nur schleppend voran. Zur Flankierung der Regelungen zum Schutz personenbezogener Daten ist daher zu prüfen, das Copyright-Recht insofern zu erweitern, jeder Person ein Copyright an ihren persönlichen Daten zu geben. Die Nutzung der Daten zu vereinbarten Zwecken ist unentgeltlich. Bei der Vermarktung von Kundendaten oder anderen personenbeziehbaren Daten, die die Schwelle des sog. fair use überschreiten, können Copyright-Gebühren im Individualfall geltend gemacht werden.

Die Kenntnis von Gefahren und Möglichkeiten, mit ihnen umzugehen, sind Grundvoraussetzungen für einen selbstbestimmten Umgang mit Informationsdienstleistungen. Von kommerziellen Interessen im Prinzip unabhängige Institutionen, die über den Schutz personenbeziehbarer Daten wachen und die Sicherheit von IT-Systemen beurteilen können, sind vorhanden. Ihr Wissen ist für die Nutzerinnen und Nutzer von Informationsdienstleistungen von hoher Bedeutung. Sie haben ihre Kenntnisse des Entwicklungsstandes ihres Gebiets fortwährend zu aktualisieren, um die Öffentlichkeit informieren zu können. Die für beides notwendigen Mittel sind ihnen bereitzustellen.

Zu B. Schutz der Verbraucherinnen und Verbraucher

Die Bundesregierung hat der Entwicklung Rechnung zu tragen, daß Anbieter digitaler und mit Hilfe von Set-top-Boxen zu empfangender TV-Kanäle schon heute mit einem Zugang zum Internet werben und auf dem Internet das laufende TV-Programm abrufbar ist. Die Anbieter arbeiten daran, die Grenzen zwischen Rundfunk und Telekommunikation aufzuheben. Die Politik kann dabei jedoch nicht abseits stehen und vereinzelte Inseln des Rechts schaffen, andere Bereiche dagegen ausgeklammert lassen.

Ohne Einmischung in Programminhalte und damit ohne Einmischung in die Länderhoheit bei den dem herkömmlichen Rundfunk nahestehenden neuen Angebotsformen einerseits und klar als Telekommunikation erkennbaren Angeboten andererseits ist auf der grundlegenden Ebene des Verhältnisses zwischen Kundinnen und Kunden und Anbietern eine einheitliche Regelung notwendig, die Kundinnen und Kunden aller Formen digitaler Dienste dieselbe Rechtssicherheit gewährt. Die Bundesregierung hat hier im Einvernehmen mit den Ländern die entsprechenden Grundlagen zu schaffen, auf denen weitere Regelungen aufbauen können, soweit sie für spezifische Dienste erforderlich sind.

Preistransparenz gehört ebenso zu den grundlegenden Eigenschaften des Verbraucherschutzes wie die Möglichkeit, einen Kauf rückgängig zu machen. Dies gilt es erst noch in die Welt digitaler Dienste zu übersetzen. Der Abrufvorgang und eine damit eingegangene Zahlungsverpflichtung hat in diesen Systemen ebenso klar und eindeutig zu erfolgen, wie in der realen Geschäftswelt, wenn es nicht zu massiven Problemen kommen soll. Die bei der Nutzung digitaler Dienste entstandenen Kosten werden heute in der Regel im laufenden Betrieb nicht angezeigt, in manchen Systemen nach Ende der Nutzung. Dabei ist auffallend, daß besonders kleine Anbieter um Kundenfreundlichkeit bemüht sind. Hier ist regulativ darauf hinzuwirken, daß die Kundinnen und Kunden zu jeder Zeit darüber informiert sind, welche Kosten ihnen durch die Nutzung entstehen und bereits entstanden sind. Einige Anbieter zeigen heute zumindest schon eine besondere Kostenpflichtigkeit von Angeboten an. Dies ist grundsätzlich vorzuschreiben für alle Kosten verursachenden Angebote, deren Abruf zudem in einer Form zu gestalten ist, die eine eindeutige Willensbekundung der Kundinnen und Kunden deutlich werden läßt. Während der Umtausch elektronischer Informationsangebote wi-

dersinnig wäre, ist das Stornieren und Widerrufen von Informationsabrufen das notwendige Instrument, dessen Umsetzung in die Form digitaler Dienste die Bundesregierung zu leisten hat.

In digitalen Diensten fehlt es mancherorts an fundamentalen Voraussetzungen kundenfreundlicher Praxis. Es gibt Verträge mit Providern von Online-Diensten, die explizit die Geltung von internationalen Mindeststandards der Allgemeinen Geschäftsbedingungen ausschließen. Andere Dienste hinterlegen ihre Geschäftsbedingungen nur elektronisch. Derartige Dokumente sind einseitig und unbemerkt leicht veränderbar und dienen nicht der Rechtssicherheit der Kundinnen und Kunden. Die Verträge und Geschäftsbedingungen sind daher in unveränderbarer Form an Kundinnen und Kunden zu übermitteln. Dies kann entweder in Papierform geschehen oder auf elektronischem Weg so organisiert werden, daß sie durch kryptographische Verfahren gegen Veränderung geschützt sind und der Eingang der elektronischen Post manuell quittiert wird. Die Bundesregierung wird aufgefordert, die Rechtslage entsprechend anzupassen.

Bei IT-Systemen wird in Kaufverträgen nicht selten die Haftung für zugesagte Eigenschaften ausgeschlossen. Digitale Dienste basieren auf derartigen Systemen. Wenn Kundinnen und Kunden einen zugesagten Preis für ihre Ware zahlen, ist endlich auch die rechtliche Grundlage zu schaffen, ihnen die zugesagte Ware und deren Eigenschaften ohne Beschränkung zu garantieren. Überdies sind die Haftungsregelungen dementsprechend weiterzuentwickeln.

Der internationale Charakter des Internets und die dabei im Zusammenhang mit unterschiedlichen Ansichten über Meinungsfreiheit auftauchenden juristischen Auseinandersetzungen sollten klargemacht haben, daß wir es mit einem elektronischen Kurzschluß von Rechtssystemen zu tun haben. Kundinnen und Kunden von Online-Shopping-Angeboten werden dies – und anders als bei Teleshopping-Kanälen – zu spüren bekommen, wenn sie Produkte und Dienstleistungen auf einem Computersystem an ihnen unbekanntem Ort bei einem Unternehmen auf der anderen Seite des Globus bestellen und dafür zahlen.

Die Nutzung derartiger Angebote wird solange unter mangelnder Rechtssicherheit leiden, wie Kundinnen und Kunden nicht dadurch normativ geholfen wird, daß die ihnen hier bekannten Rechte auch bei elektronischen Transaktionen gelten. Der beste Weg dazu ist, als Grundlage das Recht am Ort des Kunden zu bestimmen. Den Anbietern ist zuzumuten, daß sie die Rechtslage am Ort ihrer Kundinnen und Kunden kennen, Kundinnen und Kunden jedoch nicht, sich darüber zu informieren, welches Recht am Ort des Anbieters gilt und ob durch den Ort des Computersystems, über das die Transaktion abgewickelt wird, davon abweichendes Recht gilt. Die Bundesregierung ist daher gefordert, die entsprechende gesetzliche Basis zu schaffen.

Als Orientierung für Kundinnen und Kunden sowie Anreiz für Qualitätsbewußtsein und Datenschutz ist die Vergabe eines Gütesiegels vorzusehen, mit dem Anbieter von unabhängiger Seite zertifiziert werden können.

Zu C. Informationszugang und Entfaltung

Elektronische Netze wie das Internet haben deswegen einen besonderen Wert, da jede Person nicht nur Angebote konsumieren, sondern sie auch anbieten kann. Das Ergebnis ist eine beachtenswerte Vielfalt an Meinung und Aktivitäten. Vielfalt von Informationsangeboten kann nur entstehen, wenn diese nicht an unnötige Zulassungen gebunden werden. Sofern bestimmte Aspekte der Aktivitäten von Anbietern von Informationsdienstleistungen geregelt werden, hat die Bundesregierung die Interessen kleiner und nichtkommerzieller Anbieter und von Privatpersonen in besonderer Weise zu berücksichtigen und sie von solchen Maßnahmen auszunehmen, die für sie unzutreffend sind oder sie in unmäßig harter Weise treffen.

Vielfalt wird auch behindert durch den Unwillen der Bundesregierung, die von ihr mehrfach betonte Rechtslage bei Informationsdienstleistungsanbietern mit Nachdruck zu vertreten. Der Abruf von Daten unterliegt dem Fernmeldegeheimnis. Anbieter, die lediglich den Zugang zu Informationen Dritter ermöglichen, haben daher nicht das Recht, die Inhalte ihrer Kundinnen und Kunden zu prüfen, und sind damit auch nicht für die Informationsinhalte Dritter verantwortlich. Es ist Aufgabe der Bundesregierung, den Grundrechten wenigstens auf nationaler Ebene zur Geltung zur verhelfen und den Schutz des Fernmeldegeheimnisses wie der Meinungsfreiheit effektiv zu gewährleisten. Um auch dem Schaden, der dem internationalen Ansehen der Bundesrepublik Deutschland durch Aktivitäten gegen die Meinungsfreiheit auf dem Internet entstanden ist, entgegenzuwirken, wird die Bundesregierung aufgefordert, in den mit der Weiterentwicklung der Informationsgesellschaft befaßten internationalen Gremien auf Ebene der EU, der OECD und der G7-Staaten mit Nachdruck für die Wahrung der Meinungsfreiheit in digitalen Diensten einzutreten.

Der Schutz Jugendlicher vor jugendgefährdendem Material, das auf dem Internet und anderen elektronischen Netzen abgerufen werden kann, ist durch Zensur und Kontrolle von Inhalten auf diesen Netzen weder rechtlich noch technisch möglich. Einseitige nationale Regelungen zur Kontrolle von Daten internationaler Netze sind der falsche Weg. Der Zugang zu diesen Daten vollzieht sich ja in aller Regel am heimischen Computer. Technisch verfügbar sind verschiedene Systeme, die effektiv und zuverlässig den Zugang zu und die Nutzung von gängigen Heim-Computersystemen selektiv kontrollieren und bei Bedarf blockieren. Eltern können mit Hilfe einiger Systeme ihren Kindern nicht nur einen selektiven Zugang zum Internet erlauben, sondern auch das Einspielen der bisweilen nicht minder gefährlichen Computerspiele unterbinden. Aufgabe der Eltern ist es bei der Nutzung von Computertechnik schließlich auch, die Aktivitäten ihrer Kinder in verantwortungsvoller Weise zu beaufsichtigen. Es ist im übrigen bemerkenswert, daß die Bundesregierung versäumt, hier auf die Leistungen der heimischen Softwareindustrie zu verweisen. Wer gegen jugendgefährendes Material vorgehen will, muß die Urheber auch international strafrechtlich verfolgen. Dazu hilft keine Inhaltskontrolle von Datenströmen, sondern einzig und allein die Schaffung der

rechtlichen Voraussetzungen, um die Strafverfolgungsbehörden hierzulande zu einer Kooperation mit ihren Kolleginnen und Kollegen in anderen Ländern zu befähigen. Dies ist nur möglich durch polizeiliche Kooperationsabkommen und eine Angleichung rechtlicher Unterschiede in den Rechtssystemen der beteiligten Staaten.

Das Recht auf einen Zugang zu Behördendaten (Freedom of Information) ist nicht nur logische Voraussetzung für das Einstellen von Behördendaten in die geplanten Bürger-Informationssysteme, sondern ist ein längst überfälliges Zeichen demokratischer Kultur, das nicht nur in den USA, sondern auch den EU-Ländern längst Praxis ist. Das Umweltinformationsgesetz ist ein untaugliches und deshalb zu novellierendes Beispiel einer Umsetzung des Akteneinsichtrechts durch Bürgerinnen und Bürger. Es ist deshalb dahin gehend zu novellieren, den Zugang zu Daten der Verwaltungen allgemein weder durch Kosten noch durch eine Privatisierung der Datenverarbeitung von Behörden einzuschränken, sondern nur durch den Schutz der Persönlichkeitsrechte Betroffener.

Das Internet und damit auch alle kommerziellen Anbieter, die einen Zugang dazu zur Verfügung stellen, leben von Ressourcen, die Universitäten und Forschungseinrichtungen in Form von Leitungen, Software und Arbeitsaufwand zur Verfügung stellen und die vom Deutschen Forschungsnetz koordiniert und unterstützt werden. Universitäten und Forschungseinrichtungen sind zudem als Orte der Erarbeitung von Wissen auch bedeutende Produzenten von Informationen. Die Herstellung von interessanter Vielfalt, weitgehend zuverlässiger Funktion und der Entwicklung neuer Anwendungen ist nur über die fundierte Unterstützung dieser Institutionen möglich, zu der die Bundesregierung nachdrücklich aufgefordert ist.

Informationstechnische Bildung in der Schule geschieht nicht dadurch „automatisch", daß Schulen mit Informationstechnik ausgestattet werden. Dazu sind Investitionen in die dauerhafte Qualifikation der Lehrenden wie der Lernenden notwendig. Es ist mittlerweile Stand der Wissenschaft, daß Computer Lehrende nicht ersetzen, sondern – soll eine angemessene Qualität erreicht werden – mehr und entsprechend ausgebildete Lehrkräfte erfordern. Bei dem gegenwärtigen Stand der Bildungsausgaben in der Bundesrepublik Deutschland, die am Ende der OECD-Skala zu finden ist, droht gegenwärtig der Anschluß an neues Wissen verlorenzugehen, wenn in Schulen, Universitäten und bei beruflicher Qualifikation nicht hinreichend auf die Anforderungen von morgen vorbereitet wird. Die Schule ist aber nicht nur der Ort, jene Qualifikation im Umgang mit neuen Techniken zu vermitteln, die notwendig sind zur Erwerbsarbeit, mit der – zumindest vorübergehend – international konkurrenzfähige Produkte und Dienstleistungen hergestellt werden können. Bildung eröffnet auch die Möglichkeiten, um über Risiken und Chancen der neuen Informations- und Kommunikationstechnologien zu informieren. Für dies hat die Bundesregierung dauerhaft ausreichend Mittel zur Verfügung zu stellen, statt kurzfristige Programme zu konzipieren.

Zu D. Digitale Signatur und Kryptographie

Elektronische Kommunikation findet fast durchweg ohne Schutz gegen Mitlesen statt. Durch kryptographische Verfahren kann die Kommunikation aller, die dies wünschen, einfach und effektiv verschlüsselt werden. Die in der Diskussion befindlichen Verschlüsselungsstandards, deren „Sollbruchstelle" Regierungen und anderen Stellen den Zugriff auf persönliche Daten bzw. Betriebsgeheimnisse ermöglichen würden, sind eine nicht hinnehmbare Aushöhlung des Grundrechts auf Informationelle Selbstbestimmung. Sicherheitsbehörden können durchaus in ausreichender und verschiedener Weise an die benötigten Informationen von konkret Verdächtigen gelangen. Vertrauliche Kommunikation ist überdies auch im Interesse der Informationsanbieter selbst, denn Mängel im Datenschutz werden als eines der entscheidenden Hemmnisse für die Durchsetzung der Informationsgesellschaft betrachtet. Untauglich und in der Praxis nicht durchsetzbar sind deshalb alle Verfahren, die einen minderen kryptographischen Schutz deshalb gewährleisten, weil entweder die Schlüssel zu hinterlegen sind oder Sollbruchstellen in den Algorithmus eingebaut sind.

Die als Escrow-Verfahren bekannten Verteil-, Aufbewahrungs- und Zugriffsmethoden für digitale Signaturen und andere Kryptierverfahren, die dem Staat einen Zugriff auf den Schlüssel und die Identität des Signaturinhabers, aber auch die Signatur selbst geben, sind als Aufbewahrungsverfahren nicht notwendig. Dies gilt insbesondere für digitale Signaturen. Die digitale Signatur ist eine Blanko-Unterschrift unter jede beliebige Nachricht, die daher vor unbefugtem Zugriff in besonderer Weise zu schützen ist. Escrow-Verfahren laufen den Zielen digitaler Signaturen deshalb in diametraler Weise zuwider, da zwar eine digitale Signatur bei Verlust schnell neu erzeugt ist, eine für die Nutzerinnen und Nutzer nicht kontrollierbare Verfügung über digitale Signaturen durch Escrow-Verfahren aber eine Nutzung und damit Signatur von Nachrichten durch unbefugte Dritte möglich machen. Das wäre das genaue Gegenteil der damit erhofften Rechtssicherheit. Die Anforderungen an die Sicherheit reiner Beurkundungsstellen sind zudem nicht so hoch wie an Escrow-Agenturen. Sie haben lediglich eine einmalige Beurkundung und später eine zuverlässige Überprüfung zu leisten, müssen jedoch den privaten Schlüsselteil der Signatur selbst nicht verwalten.

Für digitale Signaturen bestehen keine internationalen Regelungen. Zwangsläufig haben entsprechende Regelungen entweder nur nationale Bedeutung oder setzen die Anerkennung auf der Basis freiwilliger Gegenseitigkeit voraus. Jeder kann daher im Prinzip jedem anderen eine digitale Signatur beglaubigen. Für ihren Gebrauch in der Geschäftswelt ist es allerdings nützlich, unabhängige und vertrauenswürdige Instanzen mit der Beglaubigung digitaler Signaturen und deren Bestätigung gegenüber Dritten zu beauftragen.

Die verschiedenen Nutzergruppen werden digitale Signaturen in sehr unterschiedlicher Weise nutzen wollen. Vor einer Gleichstellung digitaler Signaturen mit Papierdokumenten sind daher der Praxiseinsatz abzuwarten und die dabei gewonnenen Erfahrun-

gen wissenschaftlich zu evaluieren. Erst auf der Basis dieser Bewertung ist es sinnvoll, dauerhafte Strukturen zu schaffen.

Für die Erzeugung digitaler Signaturen sind technische und organisatorische Standards zu entwickeln, die eindeutige und nicht verfälschbare Signaturen garantieren. Die Erzeugung digitaler Signaturen kann gemäß dieser Standards entweder von geprüften Anbietern von Signaturen oder eigenverantwortlich durch die Nutzung geprüfter Software zur Signaturerzeugung durchgeführt werden. Einer Beglaubigungsstelle ist auch das zur Erzeugung verwandte Verfahren anzuzeigen, um eine Bewertung der Zuverlässigkeit der Signatur zu ermöglichen.

Druck: Thenée Druck, 53113 Bonn, Telefon 91781-0
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333